IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
v.	**:**	**CRIMINAL NO. 09 -737-01**
CHRISTOPHER ALLEN LEWIS	**:**	

UNITED STATES' PLEA MEMORANDUM

Introduction

Defendant Christopher Allen Lewis, through counsel, has indicated his desire to plead guilty to the pending indictment without a plea agreement. Lewis will plead guilty to Count 1 of the indictment, charging him with conspiracy to intentionally damage a protected computer system, in violation of Title 18, United States Code, Section 371. This charge arises from the defendant's agreement with his codefendants to disrupt the operation of the Internet website comcast.net, and from doing so by changing settings in a protected computer without authorization which caused that website to be unavailable to its subscribers for a period of time on May 28 and May 29, 2008. The Court has set a plea hearing for Wednesday, February 24, at 10:00 AM.

I. MAXIMUM PENALTIES

The Court may impose the following statutory maximum sentence on Count 1 (conspiracy): 5 years imprisonment, a $250,000 fine, three years of supervised release, restitution, and a $100 special assessment.

II. ELEMENTS OF THE OFFENSES

In order to prove a violation of 18 U.S.C. § 371, conspiracy, the government must prove the following:

(1) That two or more persons agreed to commit an offense against the United States, as charged in the indictment;

(2) That the defendant was a party to or member of that agreement;

(3) That the defendant joined the agreement or conspiracy knowing of its objective to commit an offense against the United States and intending to join together with at least one other alleged conspirator to achieve that objective; that is, that the defendant and at least one other alleged conspirator shared a unity of purpose and the intent to achieve a common goal or objective, to commit an offense against the United States; and

(4) That at some time during the existence of the agreement or conspiracy, at least one of its members performed an overt act in order to further the objectives of the agreement.

III. FACTUAL BASIS FOR PLEA

If this case were to proceed to trial, the government would prove each element of the crime charged beyond a reasonable doubt. The government's evidence would consist of both testimonial as well as physical evidence. The government would prove the following:

In May of 2008 the defendant used the name "EBK" and was a member of a hacking and phone phreaking group called "Kryogeniks." This group also included Lewis's codefendants. On approximately May 26, 2008, the defendant discussed with others in "Kryogeniks" the internet website fear.net, owned by Comcast corporation. Defendant Lewis and the other defendants in the group also decided and agreed to attempt to take control of the internet website comcast.net.

On approximately May 27, 2008, defendant Lewis placed a telephone call to a Comcast

employee at his home in Clifton Heights, Pennsylvania to see of that employee would answer questions about Comcast's fearnet.com domain.

On approximately May 27, 2008, the defendant used telephone calls to obtain information which allowed his codefendants, with his knowledge, to gain unauthorized access to an account which Comcast maintained with its provider of Domain Name System (DNS) information. With this unauthorized access, the defendant's coconspirators then successfully logged in to that account. This gave the defendants access to the DNS information for the site comcast.net, and thus gave the defendants the power to change the internet site to which internet users were directed when they connected to comcast.net. That is, it allowed the defendants to change the Internet Protocol (IP) address which was reached by using the domain name comcast.net.

On May 28, 2009, defendant Lewis participated in a conference call with codefendants Black and Nebel during which the three of them decided and agreed that they would redirect customers seeking access to the website comcast.net to a different website. They prepared this different website by having this website display a message indicating that "Kryogenics" had successfully "hijacked" the comcast.net domain name.

On or about May 28, 2008, the defendants accessed a "virtual private network" (VPN) based in Sweden and later sent computer commands through this network to the target computers. They did so in order to hide the location of the computer which codefendant Nebel was using to execute the "hijack" of comcast.net by making it seem that these computer commands came from the location of the Swedish VPN and not from the location of Nebel's computer.

At approximately 11:00 PM on or about May 28, 2008, codefendant Nebel, in conjunction with and at the direction of this defendant and codefendant Black, used the administrative access to Comcast's account with the company maintaining its DNS information to intentionally send computer code and commands to the computer controlling this DNS information, and by doing so intentionally changed the IP address to which users of the comcast.net website were directed when they signed on to this site. The defendants directed these users of comcast.net to the different website which they had prepared and which displayed the following message: "KRYOGENIKS Defiant and EBK RoXed COMCAST sHouTz to VIRUS Warlock elul21 coll1er seven." These actions impaired the availability of the of the website comcast.net for at least 90 minutes on May 28-29, 2008, and for some users for a period of time after that.

A codefendant also used this unauthorized administrative access to this account to change the publicly available contact information for comcast.net, including changing the e-mail contact information to kryogenicsdefiant@gmail,com.

On or about May 28, 2008, Lewis, in furtherance of this conspiracy, after the defendants had changed the DNS information for comcast.net, called a Comcast employee at his home in Clifton Heights, Pennsylvania, and asked the employee if his domains were working properly.

As a result of the actions of this conspiracy, Comcast corporation suffered a loss of $128,578, which was the cost of Comcast's response to the incident, of assessing damage, of restoring the system to operation, and of other consequential damages including resecuring its DNS information.

Comcast was then a corporation headquartered in Philadelphia, Pennsylvania. In May

of 2008, approximately 5 million unique users visited the comcast.net website each day. Through the comcast.net site, Comcast provided subscribers with e-mail, voice mail, and other services. The computers used to provide these services, and the computers housing the comcast.net DNS information, were computers used in interstate and foreign commerce and communication.

V. PLEA AGREEMENT

The defendant is pleading guilty without a plea agreement.

Respectfully Submitted,

MICHAEL L. LEVY
United States Attorney

_____
ALBERT S. GLENN
ALEXANDER T. H. NGUYEN
Assistant United States Attorneys

Date: February 22, 2010

CERTIFICATE OF SERVICE

I certify that on this day I caused a copy of

UNITED STATES' PLEA MEMORANDUM

to be served by mail and by e-mail on the following:

Nina Spizer
Assistant Federal Defender
Defender Association of Philadelphia, Federal Court Division
The Curtis Center Building
601 Walnut Street, Suite 540 West
Independence Square West
Philadelphia, PA 19106

ALBERT S. GLENN
Assistant United States Attorney

Date: February 22, 2010